REMARKS

Claims 1-46 were originally presented. Claims 33-36 are canceled. New claims 47-50 are added. Thus, claims 1-32 and 37-50 are now pending.

I. ISSUES NOT RELATING TO PRIOR ART

A. CLAIM OBJECTIONS

Paragraph 4 of the Office Action objects to claims 33-36 as allegedly failing to further limit the subject matter of a previous claim. Claims 33-36 are canceled herein. Therefore, the objection is believed to be moot.

B. CLAIM REJECTIONS—35 U.S.C 112

Paragraphs 5-6 of the Office Action rejected claims 1-46 under 35 U.S.C. 112.

The Office Action contended that the independent claims are unclear and indefinite for allegedly failing to recite what steps are performed if the identifier is not present. The rationale of the Office Action is incorrect and unsupported in any case law. Processing steps involved when an identifier is not present are immaterial. The claims positively recite what the applicants consider to be the invention, namely processing steps performed when an identifier is found in an encrypted packet. The present claims are allowable under the applicable statute and the case law because there is no legal requirement for an applicant's claims to recite every other logical possibility relating to a claimed process.

The Office Action rejected claims 2, 7-10, 15, 20-23, 28, 33-35, 38, and 43-46 as allegedly unclearly referring to encrypting a packet that may be already encrypted.

Present claim 2 now recites that the encrypting occurs before the examining. Thus, the encrypting step involves encrypting a packet that was not previously encrypted. Applicant believes that the rejection is overcome for claims 2 and 7-10, which depend from claim 2, and claims 15 and 20-23 which refer to claims 2 and 7-10.

Present claim 28 recites that the means for encrypting is operable before the examining means. Applicant believes that the rejection is overcome for claim 28. Claims 33-35 have been canceled.

Present claim 38 recites that the encrypting occurs before the examining. Applicant believes that the rejection is overcome for claims 38 and 43-46, which depend from claim 38.

Reconsideration is respectfully requested.

II. ISSUES RELATING TO PRIOR ART

A. CLAIMS 1-3, 5, 7, 11, 14-16, 18, 20, 24, 27-29, 31, 33, 34, 37-39, 41, 43

The Office Action rejected claims 1-3, 5, 7, 11, 14-16, 18, 20, 24, 27-29, 31, 33, 34, 37-39, 41, and 43 under 35 U.S.C. 102(e) as allegedly anticipated by Buer et al. The rejection is respectfully traversed.

A rejection under §102 is traversed if the claims recite one or more features, elements, steps or limitations that are not found in the cited reference. Stated another way, the cited reference must teach or disclose each and every feature of the claims, arranged as in the claims. *See Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983). The claims of the present application contain features not found in the reference, and therefore the rejection is overcome.

As originally filed, all independent claims recited applying a service to an encrypted packet, determining whether an identifier associated with the quality of service is present in the encrypted packet, and if the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet. Claims are interpreted in light of the specification and with the knowledge of one of ordinary skill in the art, *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582, 39 USPQ2d 1573, 1576-77 (Fed. Cir. 1996), and by reading applicants' complete specification it is clear that "service" referred to "quality of service" in networks.

Merely to make explicit what was previously implicit, present claim 1 recites a "method for applying a quality of service to an encrypted packet comprising ... examining an encrypted

packet; determining whether an identifier associated with the quality of service is present in the encrypted packet; in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet." In one embodiment, a network element could receive an encrypted packet, determine whether the encrypted packet contains an identifier that is associated with a particular quality of service treatment, and then apply the particular QoS treatment to the packet.

Therefore, QoS can be applied to encrypted packets in which QoS markings are normally impossible to read because of the encryption. The identifier could be an IKE identifier. To the best of the knowledge of the applicant, past approaches have been unable to apply QoS to encrypted packets because the encryption obscures QoS values in the packet, and no past approach has used the IKE identifier to signal a desired QoS treatment.

The Office Action relies on paragraphs 76-77 of Buer, which state:

> **[0076]** When an encrypted packet is received by the network controller/packet processor **220**, the network controller/packet processor **220** reads the identifier in the packet to determine which security association should be used with that packet (block **614**). For example, if the identifier consists of the address of the security association the network controller/packet processor **220** reads the data from that address in the database **240**. Alternatively, if the security association includes the identifier, the network controller/packet processor **220** may scan the database for a security association that contains an identifier that matches the identifier for the packet. The network controller/packet processor **220** sends the packet and the security association to the cryptographic accelerator **236** (block **616**).
>
> **[0077]** The cryptographic accelerator **236** decrypts the security association using the key stream and sends the decrypted session key to the cipher engine **424A**, **424B** (block **618**). The cipher engine **424A**, **424B** decrypts the encrypted packet using the session key (block **620**) and sends the decrypted packet back to the network controller/packet processor **220**. The network controller/packet processor **220**, in turn, sends the packet to the host processor **224** for processing (block **622**).

Any "service" described in Buer merely involves conventional decryption based on a particular security association. Buer has no description of applying a quality of service treatment to an encrypted packet based on an identifier in the encrypted packet. For at least this reason, Buer fails to anticipate claim 1.

All independent claims (1, 11, 27, 37) recite steps or apparatus elements that provide for determining whether an identifier associated with the quality of service is present in the encrypted packet, and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet, as recited in claim 1. Thus, all independent claims and all claims that depend directly or indirectly from them include the features of claim 1 that distinguish Buer.

For at least the foregoing reasons, the rejection of claims 1-3, 5, 7, 11, 14-16, 18, 20, 24, 27-29, 31, 33, 34, 37-39, 41, and 43 under 35 U.S.C. 102(e) is traversed. Reconsideration is respectfully requested.

B. CLAIMS 4, 8, 17, 21, 30, 40, 44—BUER IN VIEW OF PIPER

Paragraphs 9-10 of the Office Action reject claims 4, 8, 17, 21, 30, 40, and 44 under 35 U.S.C. 103(a) as allegedly unpatentable over Buer in view of Piper. The rejection is respectfully traversed.

The Office Action relies on Piper pp. 19-20 to show that the IKE ID comprises the identifiers recited in claim 4 and similar claims, and the use of ISAKMP in claim 8 and similar claims. However, Piper has no description or suggestion of determining whether an identifier associated with the quality of service is present in the encrypted packet, and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet, as recited in claim 1.

Thus, Piper does not cure the deficiency of Buer with respect to the preceding features, and therefore any combination of Piper with Buer cannot provide the complete invention as

recited in claim 4 or similar claims, or as recited in claim 8 and similar claims. Reconsideration is respectfully requested.

C. CLAIMS 6, 19, 32, 42—BUER IN VIEW OF ROGE

Paragraph 11 of the Office Action rejects claims 6, 19, 32, and 42 under 35 U.S.C. 103(a) as allegedly unpatentable over Buer in view of Roge. The rejection is respectfully traversed.

The Office Action relies on Roge col. 4-5, which states in part, "... processor 18 can also process information about class of service, quality of service ... and other features attributable to the packet." However, Roge has no description or suggestion of determining whether an identifier associated with the quality of service is present in the encrypted packet, and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet, as recited in claim 1. Roge's statement about processing packet information is so general and vague that it cannot provide any suggestion of the specific technique of claim 1, in which QoS is applied to encrypted packets. Further, there is no suggestion in Roge to combine processing QoS information in packets with Buer, or any technique like that of Buer. The references are disjoint. At most, a combination of Roge and Buer would provide that processes QoS information in packets, and detects identifiers in encrypted packets, but without linking those steps together to result in **applying** QoS based on a detected identifier, because there is no reason based on Roge to do so.

Further, Roge is entitled "Bit Encoded Ternary Content Addressable Memory Cell" and is classified in US class 365/168 and other subclasses of class 365. Buer is in class 380, which covers entirely different technology. A skilled artisan seeking to solve the problem of how to apply QoS to encrypted packets would have no reason to look at class 365 or references relating to TCAM cells. The artisan aware of Buer would have no reason to think about combining Buer with TCAM references. Roge is **non-analogous art** that should be removed as a reference.

For all the foregoing reasons, Roge does not cure the deficiency of Buer with respect to the preceding features, and therefore any combination of Roge with Buer cannot provide the

complete invention as recited in claim 6 or similar claims. Reconsideration is respectfully requested.

D. CLAIMS 9, 10, 12, 22, 23, 25, 35, 36, 45, 46—BUER IN VIEW OF VALENCI

Paragraph 12 of the Office Action rejects claims 9, 10, 12, 22, 23, 25, 35, 36, 45, and 46 under 35 U.S.C. 103(a) as allegedly unpatentable over Buer in view of Valenci. The rejection is respectfully traversed.

The Office Action relies on Valenci to show pre-classification of packets. However, Valenci has no description or suggestion of determining whether an identifier associated with the quality of service is present in the encrypted packet, and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet, as recited in claim 1. Since Valenci does not cure the deficiency of Buer with respect to the preceding features, and therefore any combination of Valenci with Buer cannot provide the complete invention as recited in claim 9 or other similar claims.

Regarding claim 10, the Office Action relies on Valenci paragraphs 27, 34, 35, but the only "service" alluded to in Valenci is conventional encryption or "cryptographic processing." These paragraphs of Valenci say nothing about **applying QoS treatment to a packet based on both an identifier found in the encrypted packet and its pre-classification,** as recited in claim 10 when read in combination with claim 1, or other claims similar to claim 10.

Reconsideration is respectfully requested.

E. CLAIMS 13, 26—BUER IN VIEW OF YLONEN

Paragraph 13 of the Office Action rejects claims 13 and 26 under 35 U.S.C. 103(a) as allegedly unpatentable over Buer in view of Ylonen. The rejection is respectfully traversed.

The Office Action relies on Ylonen to show copying at least one bit into a header to identify a characteristic of the packet. However, Ylonen has no description or suggestion of determining whether an identifier associated with the quality of service is present in the encrypted packet, and in response to determining that the identifier is present in the encrypted

packet, applying the associated quality of service to the encrypted packet, as recited in claim 1. Since Ylonen does not cure the deficiency of Buer with respect to the preceding features, and therefore any combination of Ylonen with Buer cannot provide the complete invention as recited in claim 13 and 26. Reconsideration is respectfully requested.

III. NEW CLAIMS

Claims 47-50 are new. Claims 47-50 recite subject matter similar to claims 7-10 but are expressed in apparatus format dependent from claim 27. Favorable consideration is respectfully requested.

IV. CONCLUSIONS

Based on the foregoing, all the present claims are in condition for allowance.

Applicants hereby petition for an extension of time under 37 C.F.R. 1.136 for any time period necessary to make this paper timely filed.

No fee is believed to be due for this paper. However, if any applicable fee is missing or insufficient, the Director is hereby authorized to charge any applicable fee to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

/ChristopherJPalermo#42056/
Christopher J. Palermo
Reg. No. 42,056

Dated: April 30, 2007

2055 Gateway Place Suite 550
San Jose, California 95110
Tel: (408) 414-1080x202
Fax: (408) 414-1076